OBGP Based QoS Analysis for Optical Virtual Private Network Connection Setup

A thesis submitted in partial fulfilment

of the requirements for the Degree of

Bachelor of Technology

In

Electronics and Communication Engineering

By

Arya Kumar Chandan

(Roll No. 110EC0161)

Under the Guidance of

Professor Santos Kumar Das

NIT Rourkela

Department of Electronics and Communication Engineering

National Institute of Technology Rourkela

Rourkela-769008, Odisha, India

MAY 2014

Dept. of Electronics and Communication Engineering

National Institute of Technology Rourkela

Rourkela-769008, Odisha, India

CERTIFICATE

This is to certify that the thesis entitled "**OBGP Based QoS Analysis for Optical Virtual Private Network Connection Setup"** submitted to the National Institute of Technology, Rourkela (Deemed University) by Arya Kumar Chandan, Roll No. 110EC0161 for the award of the Degree of Bachelor of Technology in Electronics and Communication Engineering is a record of bonafide research work carried out by him under my supervision and guidance. The results presented in this thesis has not been, to the best of my knowledge, submitted to any other University or Institute for the award of any degree or diploma. The thesis, in my opinion, has reached the standards fulfilling the requirement for the award of the degree of **Bachelor of Technology** in accordance with regulations of the Institute.

Date: - May-2014

(Prof. Santos Ku. Das)

Assistant Professor

Department of Electronics and Communication Engineering

Acknowledgement

I owe profound appreciation to the ones who have helped incredibly in finishing of this thesis.

To start of all, I do express my gratitude and am sincerely thankful to my guide-cum-advisor Prof. Santos Kumar Das for his excellent guidance, help and support throughout the project work. Despite his busy schedule and tremendous workload, he was always available to solve any of the problems. He guided me constantly and explained the required concept with great clarity.

With same spirit, I am thankful to Prof. S. Meher, H.O.D, Department of Electronics & Communication Engineering, National Institute of Technology, Rourkela for his constant support and encouragement. I am also grateful to Prof. S. K. Sarangi, Director, National Institute of Technology, Rourkela who has been a constant source of inspiration for me.

Last but not the least, I thank Mr. Amiya Kumar Samantaray, B. Tech student and all my friends for their constructive suggestions and help which helped me in my project work.

Arya Kumar Chandan

110EC0161

Abstract

In a computer network, clients work with different applications; hence there are requirement of speed, bandwidth, delay etc. The parameters are called as Quality of Service (QoS) parameters. QoS guarantees the performance in a network. To meet the growing demand of Optical Virtual Private Network (OVPN), the Internet Service Providers (ISP) should use multiple techniques which ensure the Quality of Service.

For performing data communication between nodes in a network the path to be followed should be known. In this project, BGP/OBGP protocols have been discussed and using this protocol, paths have been found between routers. Then the optimal path is found out based on the path attributes. Also the paths are examined for QoS parameters and the best path is chosen. An OVPN model has been discussed and modified for performing Routing & Wavelength Assignment (RWA) function based on QoS requirement which is expressed in terms of Q-factor and trying to achieve minimum blocking probability of path. The objective of this project is to assign best connection between nodes as per the request from clients operating with various applications.

Keywords: BGP, OBGP, Quality of Service, Optical Virtual Private Connection, Q-Factor, Blocking Probability.

Contents

List of Figures

List of Tables

List of Abbreviation

AS – Autonomous System

BGP - Border Gateway Protocol

DVMRP - Distance Vector Multicast Routing Protocol

DWDM – Dense Wavelength Division Multiplexing

EGP - Exterior Gateway Protocol

ETED - End-to-End Delay

GMPLS - Generalised Multiprotocol Label Switch

IGMP - The Internet Group Management Protocol

IGP – Interior Gateway Protocol

IS-IS - Intermediate System to Intermediate System

MED – Multi-Exit Discrimination

OBGP – Optical Border Gateway Protocol

OCR - Optical Core Router

OSPF - Open Shortest Path First

OVPN – Optical Virtual Private Network

OXC – Optical Cross Connect

PER - Provider Edge Router

PLI - Physical Layer Impairment

PMD - Polarisation Mode Dispersion

PNNI - Private Network to Network Interface

QoS - Quality of Service

RFC – Request for Comment

RIB - Routing Information Base

RWA – Routing and Wavelength Assignment

TCP – Transmission Control Protocol

TDR - Transmission Data Rate

WDM – Wavelength Division Multiplexing

Chapter-1: Introduction

The fast development of Internet and increment in real-time applications has made a need to enhance Internet Routing technology in terms of bandwidth, performance, scalability and conveyance of new functionalities. There is need for improvement in router/routing technology which can provide optimal path and support desired quality of service.

1.1 Background

Special Purpose computers called routers connect the Internet together. As data is forwarded in the Internet from one place to another, it is a router that makes the decision as to where and how the data is forwarded. The protocols that dynamically inform the routes for that particular session are routing protocols. Routing protocols use algorithms that inform routers the best paths through networks. We will discuss some of the IP network routing protocols here.

Unicasting Routing Protocols

When a single node is to be communicated in a network, then unicast routing protocol is used. Unicast is the widely used form of communication in Internet. Some examples of unicast routing protocols:

- Distance-Vector Routing Protocol-Bellman-Ford algorithm is used in Distance vector algorithms. This process assigns a cost value to the links between each node in the network. Nodes will send information from one to another point via the path that provides the lowest total cost (i.e. the sum of the costs of the links between the nodes used).
- Link-state algorithms- Dijkstra's algorithm is used when applying link-state algorithms. A graphical map of the network is the primary data is used for the nodes. Using the map, the router independently determines a path of least-cost to every other node from itself. Dijkstra's algorithm is a standard shortest paths algorithm.
- OSPF-Open Shortest Path First is an IGP that is developed for IP Networks. OSPF is a link state protocol that makes routing decisions based on the shortest path algorithm.
- BGP-Border Gateway Protocol is an Exterior Gateway Protocol (EGP) that finds paths between routers in different autonomous systems eliminating the looping in the path information.

Multicast Routing Protocols

Multicast routing protocols empowers the IP network to perform data communication between one or more than one sources to one or more than one destinations. Some examples of multicast routing protocols are:

- DVMRP-The Distance Vector Multicast Routing Protocol, defined in RFC 1075, is a routing protocol used to share information between routers to facilitate the transportation of IP multicast packets among networks. It formed the basis of the Internet's historic multicast backbone, Mbone.
- IGMP-The Internet Group Management Protocol is a communications protocol used by hosts and adjacent routers on IP networks to establish multicast group memberships. IGMP is an fundamental part of IP multicast.

In this thesis we will discuss about BGP protocol and its extension OBGP protocol. Along with these protocols we will consider the contribution of Quality of Service parameters for finding the paths.

Quality of Service

Quality of service (QoS) is the overall performance of a telephony or computer network, especially the performance seen by the clients of the network. To measure quality of service quantitatively, several related parameters of the network are often considered, such as error rates, bandwidth, throughput, transmission delay, availability, jitter, etc. Quality of service is particularly important for the transmission of packets with special prerequisites. We will consider the bandwidth requirement and delay introduced in the path in terms of Q-factor.

1.2 Proposed Work

Previously a significant amount work has been done in the areas of BGP protocol, but less work has been done in the field of OBGP protocol and QoS. Here in this thesis we have discussed BGP protocol and implemented it using MATLAB programming for simulating the network model. We have also discussed an OVPN model and introduced some comparisons for finding the optimal path between nodes in an optical network.

1.3 Organisation of the Thesis

The rest of the thesis is organised as follows:

- Chapter 2 describes about BGP protocol and contains the simulation and results obtained from MATLAB implementation of it.
- Chapter 3 describes about OBGP.
- Chapter 3 discusses different QoS parameters and techniques for QoS.
- Chapter 5 contains the discussion of OVPN model and provisioning of paths based on QoS parameters along with simulation results.
- Chapter 6 concludes the work

Chapter 2: Border Gateway Protocol

Routing includes two basic functions.

i. Determination of optimized routing paths
ii. The transport of information groups (called as packets) through an internetwork.

One protocol that handles the process of path determination in the current networks is the Border Gateway Protocol (BGP). BGP performs inter domain routing in Transmission-Control Protocol/Internet Protocol (TCP/IP) networks.

2.1 Introduction

Border Gateway Protocol (BGP) [5] is a standardized Exterior Gateway Protocol (EGP) designed to exchange routing and reachability information between autonomous systems (AS) on the Internet. BGP was developed to replace its predecessor, Exterior Gateway Protocol (EGP) which is rarely used now, as the standard exterior gateway-routing protocol used in the global Internetwork.

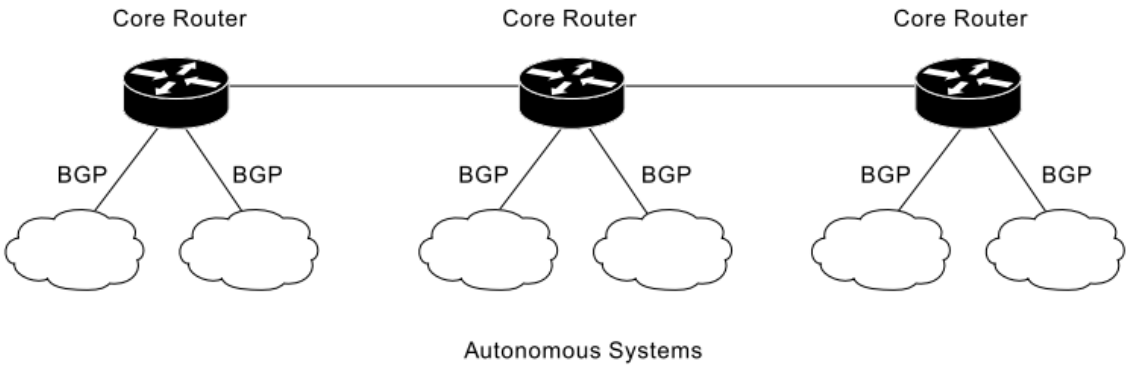

Fig 2.1- Core routers can use BGP to route traffic between autonomous systems.

BGP is specified in several Request For Comments (RFCs):

- RFC 1771—Describes BGP4, the current version of BGP
- RFC 1654—Describes the first BGP4 specification
- RFC 1105, RFC 1163, and RFC 1267—Describes versions of BGP prior to BGP4

BGP maintains routing tables, transmits routing update messages, and takes routing decisions on routing attributes. The fundamental function of a BGP system is to share network-reachability information, including information about the list of autonomous system paths, with other BGP systems. Each BGP router maintains a routing table that lists all possible paths to a particular point in the network.

2.2 BGP Operation

BGP performs three types of routing:

i. Inter-autonomous system routing
ii. Intra-autonomous system routing
iii. Pass-through autonomous system routing

Inter-autonomous system routing

- Occurs between two or more BGP router in different autonomous system.
- Peer routers in these systems use BGP to maintain a consistent view of the internetwork topology.
- BGP neighbours communicating between autonomous systems must reside on the same physical network.
- Many of these domains represent the various institutions, corporations, and entities that make up the Internet.

Intra-autonomous system routing

- Occurs between two or more BGP routers located within the same autonomous system.
- Peer routers within the same autonomous system use BGP to maintain a consistent view of the system topology.
- BGP also is used to determine which router will serve as the connection point for specific external autonomous systems.
- An organization, such as a university, could make use of BGP to provide optimal routing within its own administrative domain or autonomous system. The BGP protocol can provide both inter- and intra-autonomous system routing services.

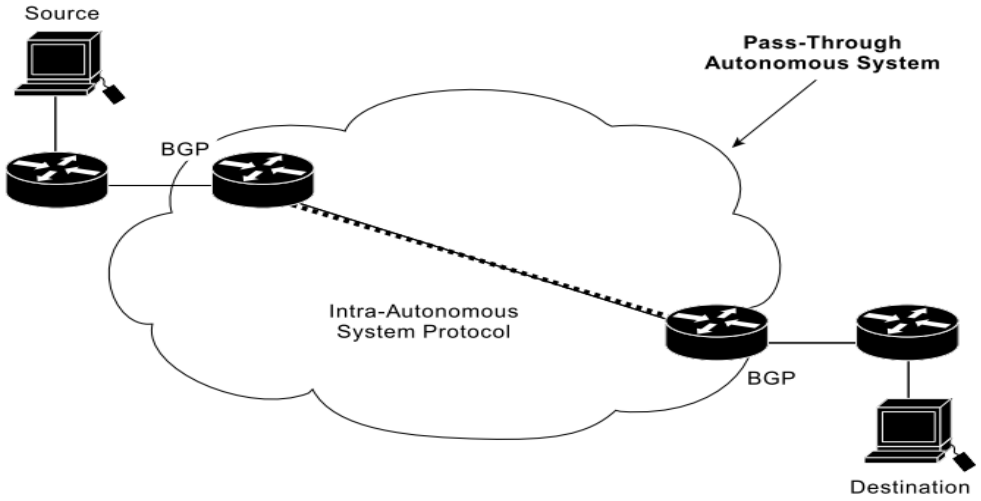

Fig 2.2 - In pass-through autonomous system routing, BGP pairs with another intra-autonomous system-routing protocol.

Pass-through autonomous system routing

- Occurs between two or more BGP peer routers that exchange traffic across an autonomous system that does not run BGP.
- BGP traffic did not originate within the autonomous system in question and is not destined for a node in the autonomous system.

2.3 BGP Message Types

Four BGP message types are specified in RFC 1771 (BGP-4). [5]

i. Open message
ii. Update message
iii. Notification message
iv. Keep-alive message

Open Message

- The open message starts a BGP communications session between nodes and is the first message sent by each side after a transport-protocol connection is established.
- Open messages are confirmed using a keep-alive message sent by the peer device and must be confirmed before updates, notifications, and keep-alive messages can be exchanged.

Update Message

- An update message is used to provide routing updates to other BGP systems, allowing routers to create a consistent view of the network model.
- Updates are sent using the Transmission-Control Protocol (TCP) to ensure reliable delivery.
- Update messages can eliminate one or more unfeasible routes from the routing table and simultaneously can advertise a route while withdrawing others.

Notification Message

- The notification message is sent when an error condition is detected.
- Notifications are used to close an active session and to inform any connected routers of why the session is being closed.

Keep-alive Message

- The keep-alive message notifies BGP peers that a device is active.
- Keep-alive messages are sent often enough to keep the sessions from entering into expire state.

2.4 BGP Path Attributes

When a BGP speaker receives updates from multiple AS that describe different paths to the same destination, it must choose a single best path for reaching that destination. The decision is based on the value of attributes [17][2] that the update contains. Here we describe the important path attributes that are used in path finding process:

- Next Hop
- Local Preference
- AS Path
- Origin
- Multi Exit Discriminator (MED)
- IGP value

Next Hop

- The BGP next hop attribute is the IP address of the next hop that is going to be used to reach a certain destination.
- BGP specifies that the next hop of EBGP-learned routes should be carried without modification into IBGP.

Local Preference

- When there are multiple paths to the same destination, the local preference attribute indicates the preferred path.
- The path with the higher preference is preferred.

AS Path

- Whenever an update passes through an AS, BGP prepends its AS number to the update.
- The AS-path attribute is the list of AS numbers that an update has traversed in order to reach a destination.
- Useful to detect and prevent loops.
- AS length can be used to select among routes unless a local preference attribute overrides.
- The path with the minimum AS length is preferred.

Origin

- The origin attribute provides information about the origin of the route. The origin of a route can be one of the three values:
    - IGP- The route is interior to the originating AS.
    - EGP- The route is learned via the Exterior Gateway Protocol (EGP).

- Incomplete- The origin of the route is unknown or learned by static configuration.

- The best path selection is according to the preferences of the origin values. The first, second and third preferences are IGP, EGP and Incomplete respectively.

Multi-Exit Discriminator

- The Multi-Exit Discriminator (MED) attribute is a hint to external neighbours about the preferred path into an AS when there are multiple entry points into the AS.
- A lower MED value is preferred over a higher MED value.
- The default value of the MED attribute is 0.
- MED is an Inter-AS-Metric.
- MED attribute that comes into an AS does not leave the AS.

IGP

- It is like local preference, but additive in nature.
- The lower value is preferred.
- It works within the AS.

2.5 BGP Routing

In the IP network each node has an IP address. The IP address is used for updating the paths between nodes in same AS as well as neighbouring AS. From fig 2.3, we can see that the routers in a single AS are working with Interior BGP (IBGP) and routers from different AS are communicating through Exterior BGP (EBGP).

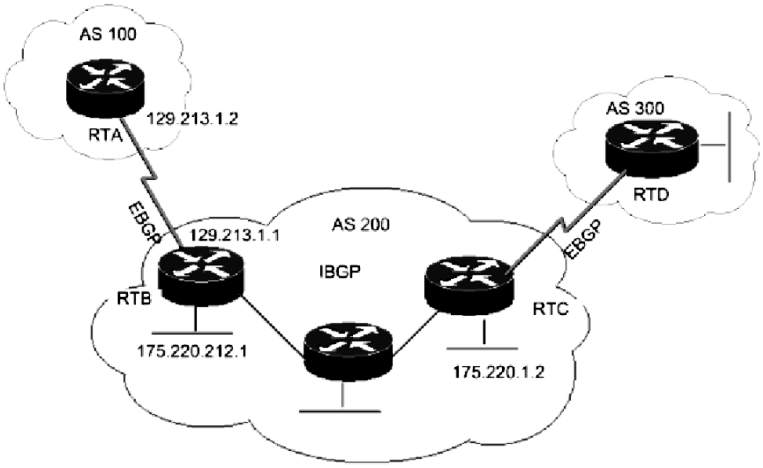

Fig 2.3 - IP network working with BGP protocol

An IP network can be modelled as follows [2]:

$G = \{AS_n, Adj, Rel\}$

Where AS_n – Autonomous System number.

Adj – Connectivity between a pair of autonomous systems.

Rel – Type of relation that exists between AS pairs.

Two types of relations are defined. Customer-to-provider relationship & peer-to-peer relationship.

The Autonomous System can be expressed in terms of the routers in it and connectivity between them as follows:

$AS_i = (V,E,P)$

Where *V* – Set of BGP speaking routers in the AS (considered as nodes)

E – Set of edges referring to the connectivity between nodes

P – Set of policies for finding the path (*NH, LP, AS_path, Origin, MED value, IGP*)

An Adjacency matrix can be obtained for the nodes in the network. It can have values as follows:

A (i,j) = { 1, if V_i and V_j are connected and 0, if no connection is there}

Route Selection Algorithm Using BGP Techniques

Different routes are learned from neighbouring peers for a single destination through update messages. From them one path is chosen based on BGP Path attributes.

Let $V_0, V_1, V_2, \ldots. V_{n-1}$ be n number of nodes in a route where source = V_i and destination = V_o

Let at node *Vi, R= {r1,r2,……}* be a collection of routes stored.

Comparison between *r1* and *r2* is made as follows:

i. If next hop is active then continue to next step; otherwise discard the current route.
ii. If *r1* and *r2* are the routes for same destination, and if (*r1.nexthop* != *r2.nexthop*), then
    a) If (*r1.loc_pref* != *r2.loc_pref*), pick route with highest Local Preference.
    b) Else pick the path that was originated by the local router.
    c) If the above are not satisfied, if (*r1.ASPath* != *r2.ASPath*), pick route with shortest AS Path length.
    d) Else if (*r1.MED* != *r2.MED*), pick route with smallest MED.
    e) Else if (*r1.IGP* != *r2.IGP*),pick route with smallest IGP value.

Flow Chart

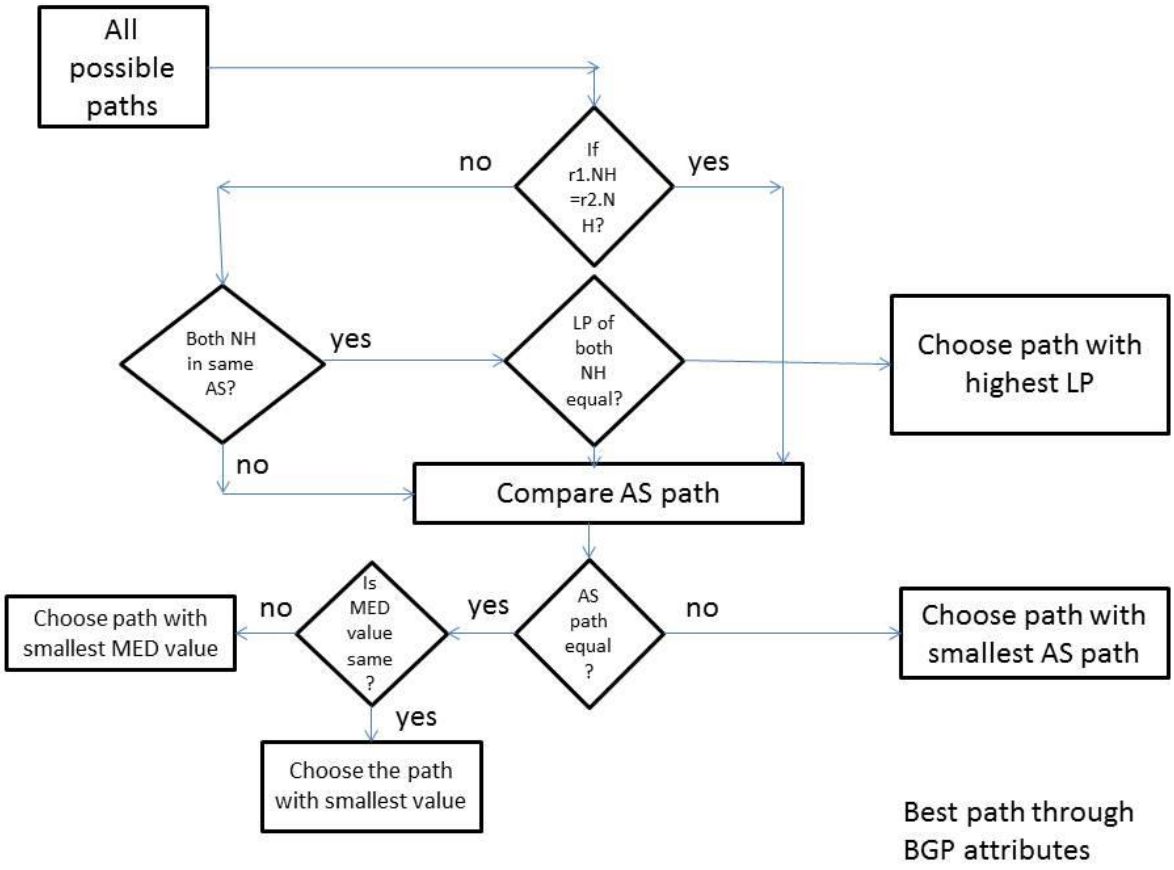

Fig 2.4 – flow chart for finding best path through BGP attributes

2.6 Simulation and Results

As we have discussed earlier an IP network can be modelled as a group of nodes in a graphical layout, we will consider the above discussed model for simulation. Here we have implemented the model using MATLAB programming. The example of network model used for simulation here is:

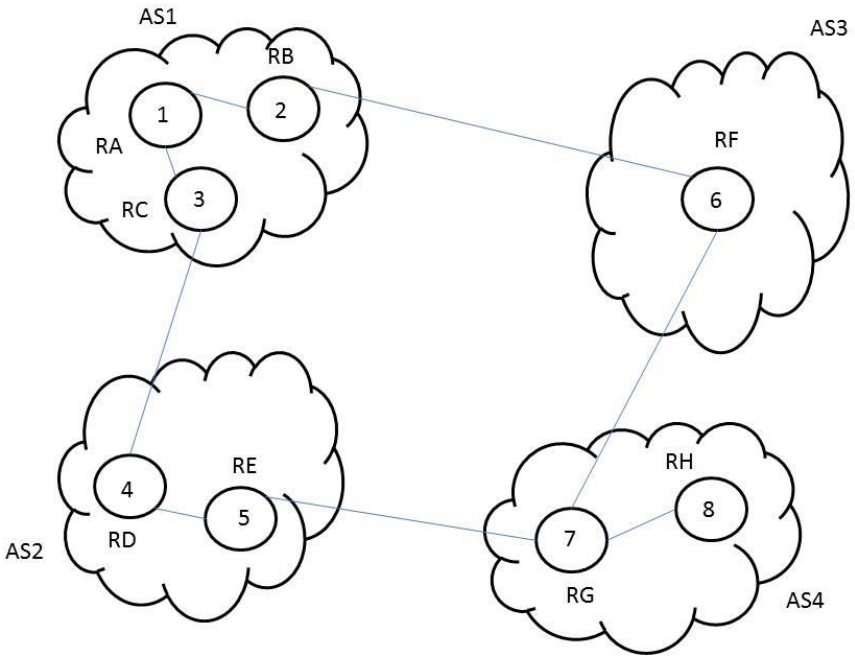

Fig 2.5 - Network model Used for simulation

The adjacency matrix and attributes matrix are given as input to the MATLAB code.

The adjacency matrix is:

	RA	RB	RC	RD	RE	RF	RG	RH
RA	0	1	1	0	0	0	0	0
RB	1	0	0	0	0	1	0	0
RC	1	0	0	1	0	0	0	0
RD	0	0	1	0	1	0	0	0
RE	0	0	0	1	0	0	1	0
RF	0	1	0	0	0	0	1	0
RG	0	0	0	0	1	1	0	1
RH	0	0	0	0	0	0	0	1

Table 2.1 – Adjacency Matrix of the example Used for BGP path finding

The attribute matrix is:

	Router	AS	AS No.	LP	IGP	MED
1	RA	AS1	1	30	25	0
2	RB	AS1	1	30	40	0
3	RC	AS1	1	30	25	0
4	RD	AS2	2	30	25	0
5	RE	AS2	2	30	25	0
6	RF	AS3	3	30	40	0
7	RG	AS4	4	30	25	0
8	RH	AS4	4	30	25	0

Table 2.2 – Attribute Matrix of the example Used for BGP path finding

Here it is assumed that the routers are having equal Local preference value. And the default MED value is 0.

Simulation – 1

(source, destination) = (1,5)

Route no.	Route path	Next Hop	LP	Origin	AS path	IGP value
1	RA,RC,RD,RE	RC	30	IGP	AS1,AS2	25
2	RA,RB,RF,RG,RE	RB	30	IGP	AS1,AS3,AS4,AS2	40

Table 2.3 – Paths between the source and destination in the example-1 with attributes

Best Path

RA,RC,RD,RE	RC	30	IGP	AS1,AS2	25

Table 2.4 – Best path obtained through algorithm in example-1

Here we have taken (source, destination) pair (1,5). Table 2.3 displays all the feasible paths between source node RA and destination node RE. In the route-1 the next hop is RC and in the route-2 the next hop is RB. As the local preferences are assumed to be same and both the next hop are from a single AS i.e. AS1, the algorithm will check for the AS path length. From the table it is learned that the route-1 is having smaller AS path as compared to route-2. So route-1 will be chosen as the optimal path.

Simulation – 2

(source, destination) = (3,7)

Route no.	Route path	Next Hop	LP	Origin	AS path	IGP value
1	RC,RD,RE,RG	RD	30	EGP	AS1,AS2,AS4	25
2	RC,RA,RB,RF,RG	RA	30	IGP	AS1,AS3,AS4	40

Table 2.5 - Paths between the source and destination in the example- 2 with attributes

Best Path

2	RC,RA,RB,RF,RG	RA	30	IGP	AS1,AS3,AS4	40

Table 2.6 – Best path obtained through algorithm in example-2

Here we have taken (source, destination) pair (3, 7). Table 2.5 displays all the feasible paths between source node RC and destination node RG. In the route-1 the next hop is RD and in the route-2 the next hop is RA. As both the next hop nodes are not from a single autonomous system, the path which starts from the router of own AS will be preferred. The source node is in AS1. The next hop in route-1 i.e. RD is in AS2 whereas the next hop in route-2 i.e. RA is in AS1, same autonomous system of as source. So, the route-2 will be preferred as the optimal path.

2.7 Conclusion

BGP is an efficient protocol for finding the best feasible path between nodes in a network. We have discussed various path attributes that are used in the process path finding here and implemented a BGP model using MATLAB programming. But, the IP network we have considered is connected with each other with electrical paths through which electrical signals can be sent. Now-a-days a high speed communication channel optical fiber is used for data communication through which light signal is transferred. So, an extended version of BGP protocol i.e. Optical Border Gateway Protocol (OBGP) is used for provisioning of paths in optical network. OBGP is studied and discussed in the next chapter.

Chapter-3: Optical Border Gateway Protocol

Optical Border Gateway Protocol (OBGP) is an extension version of Border Gateway Protocol (BGP). Due to the use of optical router in the network, a new protocol is required which can be compatible with both BGP speakers connected with each other through electrical path and routers connected through optical fiber path with each other. OBGP fulfils the above requirement.

3.1 Introduction

The Optical Border Gateway Protocol (OBGP) is an extension to BGP for manipulating Optical Cross Connects (OXCs) to permit them to be automatically setup and configured as BGP speaking devices to support multiple direct optical lightpaths among many different Autonomous Systems (ASs) [4][8]. With the large number of adjacencies possible using OBGP, lightpaths themselves may be used as a direct peering and transit mechanism between consenting ISPs.

Interconnection and direct peering also allow the enterprise or small ISP network to bypass the traditional hierarchical carriers and ISPs to establish direct peering with destination ISPs. One possible solution is to treat each OXC as a direct path between a pair of OBGP speakers. The alternative solution is to treat each OXC as an independent virtual BGP router with one input port and one output port. A virtual BGP router can then be set up for each OXC and separate OBGP sessions are initiated with peers of the virtual BGP router.

If AS paths fluctuate frequently — a phenomenon called route flapping — then the virtual BGP routers spend a great deal of time to update their routing tables and to propagate the routing changes.

3.2 Architecture of OBGP

There are two approaches for inter-domain optical networking,

i. BGP/GMPLS
ii. OBGP

BGP/GMPLS

The Generalised Multiprotocol Label Switch (GMPLS) architecture extends MPLS signalling protocols to circuit switched network.

OBGP

OBGP is intended to allow customers to control the routing of their lightpaths through another entity's optical wavelength cloud. A carrier may have a large managed wavelength cloud, but rather than hiding the routing of the wavelengths from the customer, the customer may be given a limited view of the network topology or a choice of possible routes which are subsets of all possible routes. OBGP allows the customer's topology to take precedence over the carrier's preferred topology.

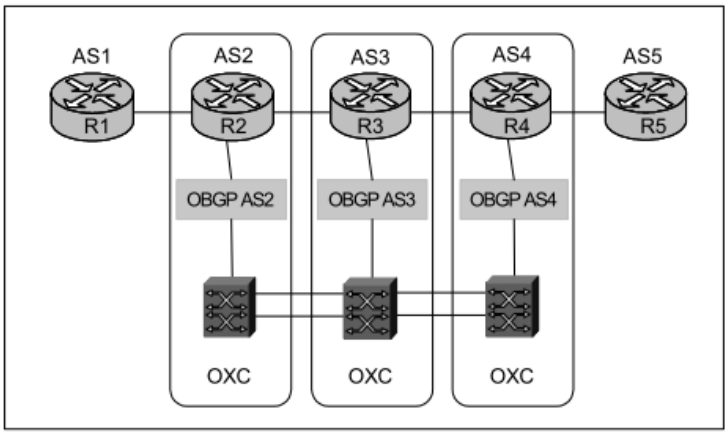

Fig 3.1 - OBGP configuration in optical Internet.

OBGP routers with multiple paths in the OXC path are given preference over any path that goes through an electrical forwarding engine using standard BGP techniques for selecting the shortest AS path, local preferences, and such.

There are two ways to configure Router B. One is to treat each OXC as a direct path between a pair of BGP speakers. However, this significantly increases the complexity of any single BGP session, particularly for many parallel lightpaths.

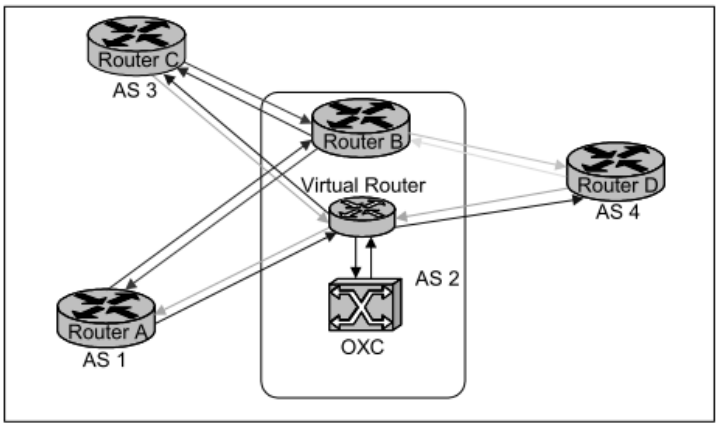

Fig 3.2 - Virtual router for OBGP.

Another is to treat each OXC as an independent virtual BGP router with only one input port and one output port. A virtual BGP router can then be set up for each OXC and separate BGP sessions initiated with its peers.

A number of mechanisms have been proposed for the management and control of such wavelength cloud systems. Most of these systems have been designed on variations of link state interior routing protocols, such as

- OSPF (Open Shortest Path First)
- IS-IS (Intermediate System to Intermediate System)
- PNNI (Private Network to Network Interface)
- complementary extensions of MPLS, such as GMPLS

3.3 OBGP Operation

The main operation of OBGP consists of two phases [4].

The first phase is the lightpath reachability phase. During this phase, sites advertise the availability of the optical lightpath to their sites through BGP. These announcements contain information on the OXC and the available lightpath through the OXC. This first phase allows sites to build up a lightpath Routing Information Base (RIB) that is used to determine if a lightpath is available across a number of OXCs in different sites.

The second phase is the lightpath establishment. This phase uses the information received from the lightpath reachability phase and then uses a BGP UPDATE message to communicate the lightpath establishment to the OXC sites on the path.

Chapter-4: Quality of Service

A stream of packets from a source to a destination is called a flow. In a connection-oriented network, all the packets belonging to a flow follow the same route; in a connectionless network, they may follow different routes. The needs of each flow can be characterized by four primary parameters: reliability, delay, jitter, and bandwidth [16][9]. Together these determine the QoS (Quality of Service) the flow requires.

4.1 QoS Parameters

Application	Reliability	Delay	Jitter	Bandwidth
E-mail	High	Low	Low	Low
File transfer	High	Low	Low	Medium
Web access	High	Medium	Low	Medium
Remote login	High	Medium	Medium	Low
Audio on demand	Low	Low	High	Medium
Video on demand	Low	Low	High	High
Telephony	Low	High	High	Low
Videoconferencing	Low	High	High	High

Table 4.1 – Stringent requirements of QoS parameters for various applications

The first four applications have stringent requirements on reliability. No bits may be delivered incorrectly. This goal is usually achieved by doing checksum operation at each packet and verifying the checksum at the destination. If a packet is damaged in transit, it is not acknowledged and will be retransmitted eventually. This strategy gives high reliability. The four final (audio/video) applications can tolerate errors, so no checksums are computed or verified.

File transfer applications, including e-mail and video, are not delay sensitive. If all packets are delayed uniformly by a few seconds, no harm is done. Interactive applications, such as Web surfing and remote login, are more delay sensitive. Real-time applications, such as telephony and videoconferencing have strict delay requirements. If all the words in a telephone call are each delayed by exactly 2.000 seconds, the users will find the connection unacceptable. On the other hand, playing audio or video files from a server does not require low delay.

The first three applications are not sensitive to the packets arriving with irregular time intervals between them. Remote login is somewhat sensitive to that, since characters

on the screen will appear in little bursts if the connection suffers much jitter. Video and especially audio are extremely sensitive to jitter. If a user is watching a video over the network and the frames are all delayed by exactly 2 seconds, no harm is done. But if the transmission time varies randomly between 1 and 2 seconds, the result will be terrible. For audio, a jitter of even a few milliseconds is clearly audible.

Finally, the applications differ in their bandwidth needs, with e-mail and remote login not needing much, but video in all forms needing a great deal.

4.2 Techniques Used for QoS

Following are some of the techniques discussed. These are used to achieve QoS [16] in optical networking.

Overprovisioning

An easy solution is to provide so much router capacity, buffer space, and bandwidth that the packets just fly through easily. The trouble with this solution is that it is expensive. To some extent, the telephone system is overprovisioned.

Buffering

Flows can be buffered on the receiving side before being delivered. Buffering them does not affect the reliability or bandwidth, and increases the delay, but it smoothers out the jitter. For audio and video on demand, jitter is the main problem, so this technique helps a lot.

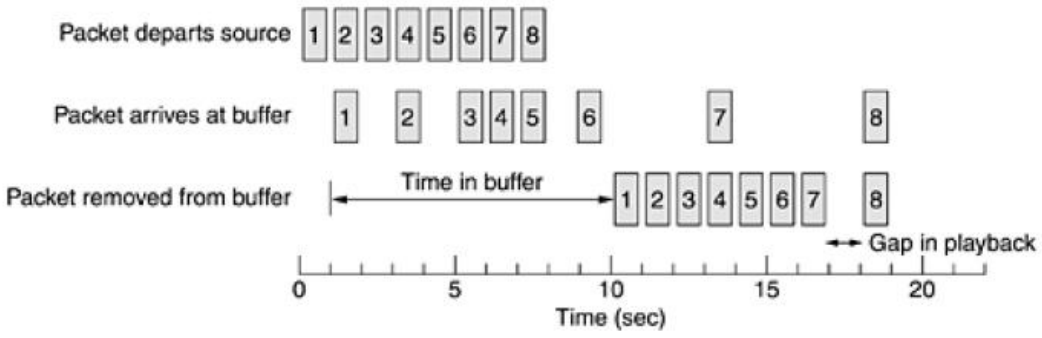

Fig 4.1 – smoothing the output packets by buffering

Packet 1 is sent from the server at t = 0 sec and arrives at the client at t = 1 sec. Packet 2 undergoes more delay and takes 2 sec to arrive. As the packets arrive, they are buffered on the client machine. At t = 10 sec, playback begins. At this time, packets 1 through 6 have been buffered so that they can be removed from the buffer at uniform intervals for smooth play.

Traffic Shaping

Traffic shaping is about regulating the average rate (and burstiness) of data transmission. In contrast, the sliding window protocols we studied earlier limit the amount of data in transit at once, not the rate at which it is sent. When a connection is set up, the user and the subnet (i.e., the customer and the carrier) agree on a certain traffic pattern (i.e., shape) for that circuit. Sometimes this is called a service level agreement. As long as the customer fulfils her part of the bargain and only sends packets according to the agreed-on contract, the carrier promises to deliver them all in a timely fashion. Traffic shaping reduces congestion and thus helps the carrier live up to its promise. Such agreements are not so important for file transfers but are of great importance for real-time data, such as audio and video connections, which have stringent quality-of-service requirements.

The leaky Bucket Algorithm

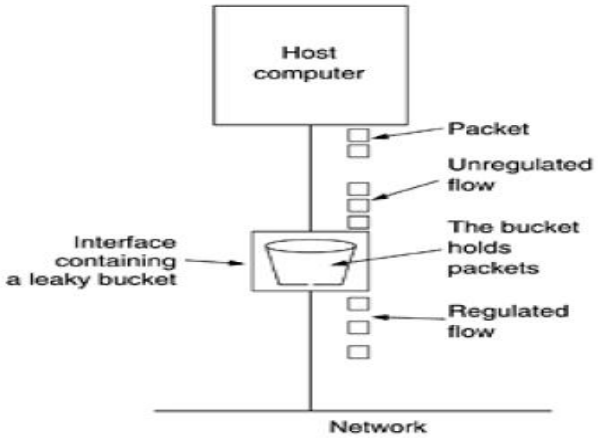

Fig 4.2 – Leaky Bucket Algorithm

Conceptually, each host is connected to the network by an interface containing a leaky bucket, that is, a finite internal queue. If a packet arrives at the queue when it is full, the packet is discarded. In other words, if one or more processes within the host try to send a packet when the maximum number is already queued, the new packet is unceremoniously discarded. This arrangement can be built into the hardware interface or simulated by the host operating system. It is called the leaky bucket algorithm. In fact, it is nothing other than a single-server queuing system with constant service time.

Chapter-5: Optical Virtual Private Network

5.1 Introduction

A VPN is a virtual network since it is not built physically and separately, but it is only a split and allocated parts of resources of a public network of a provider. It is private since it serves a closed group of users. It performs the RWA (Routing & Wavelength Assignment) function of taking data from its source to destination.

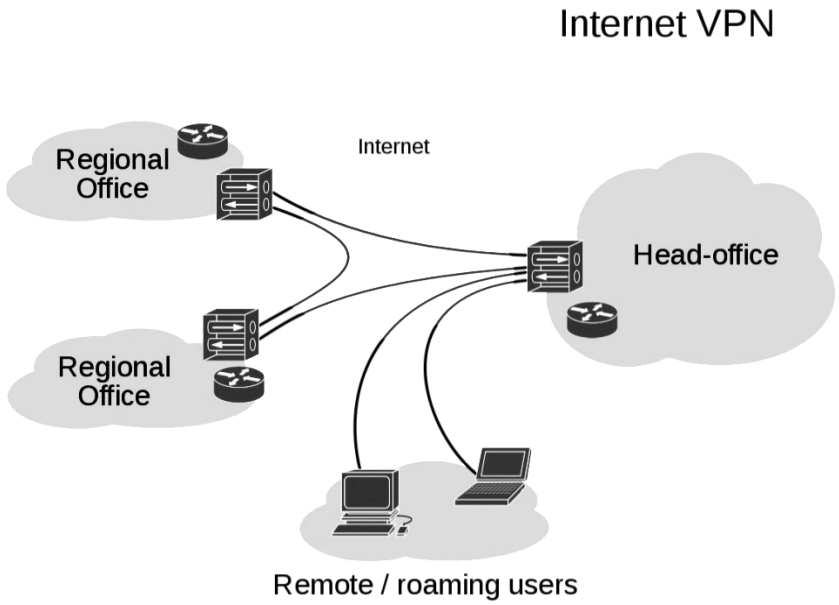

Fig 5.1 – overview of VPN

The IP based virtual private network (VPN) can realize only point-to-point connection oriented services. In Optical Virtual Private Network the connections are done with optical fiber communication channel.

5.2 OVPN Model

An OVPN system model [1] is discussed here. The model is shown in the fig 5.2. A node in the network might be a redistribution point or an end point for communication. Link is the connectivity between two nodes in the network. This model works with the concept of Wavelength Division Multiplexing (WDM/DWDM) over VPN. The clients are specified by various QoS requirements, such as Transmission Data Rate (TDR), End-to-End Delay (ETED) or Q-factor.

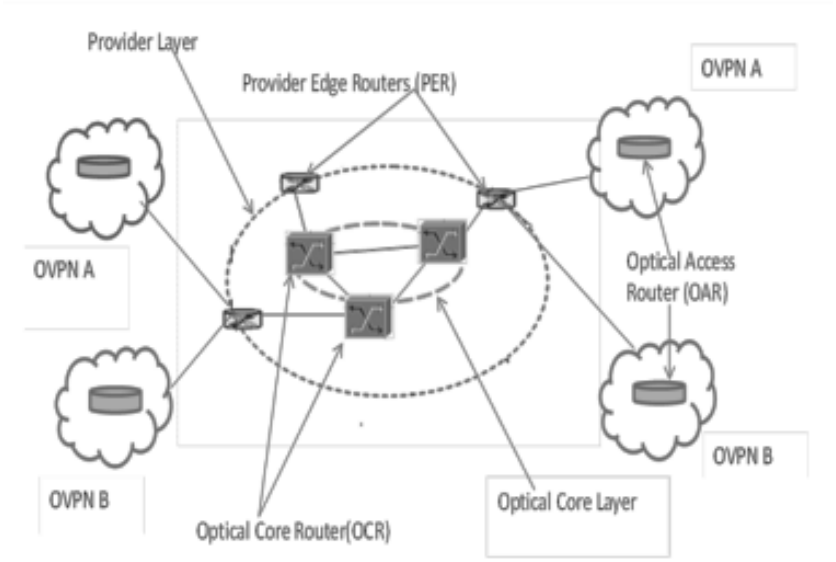

Fig 5.2 – The OVPN system model

This network model consists of two layers: the Provider edge layer and the Optical core layer. Provider Edge Router (PER) belongs to an OVPN client which provides OVPN service and interface between client and Optical Core Router (OCR). An OCR is not connected to a client directly. The optical layer provides point-to-point connectivity between routers in the form of fixed bandwidth circuits, which is termed as light-paths. In provider layer the PER are responsible for all the non-local management functions such as management of optical resources, configuration and capacity management, addressing, routing, topology discovery, traffic engineering, and restoration etc.

5.3 QoS in OVPN

As the connections in OVPN are of optical fiber paths, so there will be requirement of bandwidth for various applications. As the light travels through the optical fiber, it is a flow of pulses representing 1 & 0 for presence and absence of light respectively. Gradually, it starts to spread in pulse width thus occurrence of chromatic dispersion. Also there is physical medium dispersion which is caused by torsion, heat of the environment. So there will be delay in transmission.

QoS parameters in OVPN connection setup are: bandwidth, differential time delay, physical layer impairment (PLI) constraints, dispersion, jitter, spectral width and wavelength of light. Here we will consider the bandwidth requirement and delay parameters for provisioning of paths in OVPN. QoS requirements can be expressed in a term defined as Q-factor. The Q-factor can be defined as the ratio of bandwidth required to the delay introduced in the path.

5.4 Estimation & Computation of Q-factor

The network can be modelled as nodes and links in a graphical layout which can provide the interconnection between routers in the network. The connectivity in the network can be expressed as the adjacency matrix, which can have values as '1' if there is a connection between two nodes and '0' if there is no connection. The path allotment process in OVPN is based on the required Q-factor and provided Q-factor by the path. Here we will discuss some parameters for understanding the provisioning process in the OVPN. Such as:

- Required Q-factor
- Computed Q-factor
- Blocking probability

We will discuss optimization of the OVPN based on the parameters.

Required Q-Factor

This parameter is a QoS requirement from the client and it depends on the application running on the client side. The Q-factor can be defined as the ratio of bandwidth required from the client to the delay required.

Suppose an application for an OVPN client m and n of source-destination pair (s, d) has bandwidth requirement of B (m, n, s, d) and the delay requirement of D (m, n, s, d). Then the required Q-factor can be calculated as

$$QF_r(m,n,s,d) = \frac{B(m,n,s,d)}{D(m,n,s,d)}$$

Computed Q-factor

Here we have taken assumption of the physical layer constraints as Polarisation Mode Dispersion (PMD) [1][3] and link length. We have considered PMD for the delay calculation as it is the significant factor for generating delay in the fiber path.

Polarisation Mode Dispersion- In an ideal optical fiber, the core has a perfectly circular cross-section. In this case, the fundamental mode has two orthogonal polarizations (orientations of the electric field) that travel at the same speed. The signal that is transmitted over the fiber is randomly polarized, i.e. a random superposition of these two polarizations, but that would not matter in an ideal fiber because the two polarizations would propagate identically.

In a realistic fiber, however, there are random imperfections that break the circular symmetry, causing the two polarizations to propagate with different speeds. In this case, the two polarization components of a signal will slowly separate, e.g. causing pulses to spread and overlap. Because the imperfections are random, the pulse spreading effects

correspond to a random walk, and thus have a mean polarization-dependent differential time delay D_{PMD} (I, j) proportional to the square root of propagation link length L (I, j)

$$D_{PMD}(i,j) = DS_{PMD}(i,j) \times \sqrt{L}(i,j)$$

DS_{PMD} is the PMD parameter of the fiber, typically measured in ps/√km.

The bandwidth matrix B (i, j) for can be defined

$$B(i,j) = \frac{\sigma}{DS_{PMD}(i,j) \times \sqrt{L(i,j)}}$$

Where σ represents the pulse broadening factor. The value should typically be less than 10% of a bit time slot for which polarization mode dispersion can be tolerated.

The computed Q-Factor for a link of (source, destination) pair i and j, QF (i, j) is

$$QF(i,j) = \frac{B(i,j)}{D_{PMD}(i,j)}$$

If p(s, d) is the OVPN connection path for a source (s) and destination (d) pair, then computed Q-Factor

$$QF_C(m,n,s,d) = Min\{QF(i,j)\}, \forall (i,j) \in p(s,d)$$

Where i and j are node pair in a link.

Optimised OVPN Connection Setup

The connections are optimised based on the required Q-factor and computed Q-factor. If the required Q-factor is matched by any of the connections then a connection is provided to it; otherwise no connection is made.

Suppose, there are N number of OVPN connections for a given source S and destination D pair. The computed Q-factor will be

$$QF_c(m,n,s,d) = Max\{QF(OVPN^k_{(m,n,s,d)})\},$$

$$\forall\, k \in \{1,2,\ldots\ldots,N\}$$

Where $OVPN^k(m,n,s,d)$ - k^{th} OVPN connection

The required condition for allotting paths is:

$QF_r(m,n,s,d) <= QF_c(m,n,s,d)$

The request is blocked in two cases:

Case-1:- $QF_r(m,n,s,d) > QF_c(m,n,s,d)$

Case-2:- Wavelength is not available.

5.5 Connection Setup Algorithm & Flow chart

OVPN Connection Setup Using Shortest Path

STEP 1: Find all possible OVPN connections for a connection request.

STEP 2: Find the Shortest Distant OVPN connection from all possible OVPN connections s and computed Q-Factor.

STEP 3: Compare the required Q-Factor value of the connection request to the computed Q-Factor value of the OVPN obtained in STEP3.

STEP 4: If it is satisfied then go to STEP 5, otherwise go to STEP 7.

STEP 5: Check whether the selected OVPN is busy or not. If busy the call will be blocked. Go to STEP 1 for next connection request, otherwise go to STEP 7.

STEP 6: The call is blocked. Go for next connection request. Go to STEP 1.

STEP 7: Assign the selected OVPN connection to the requested connection. Go to STEP 1 for next connection request.

The algorithm [1] can be better understood with the help of the flow chart

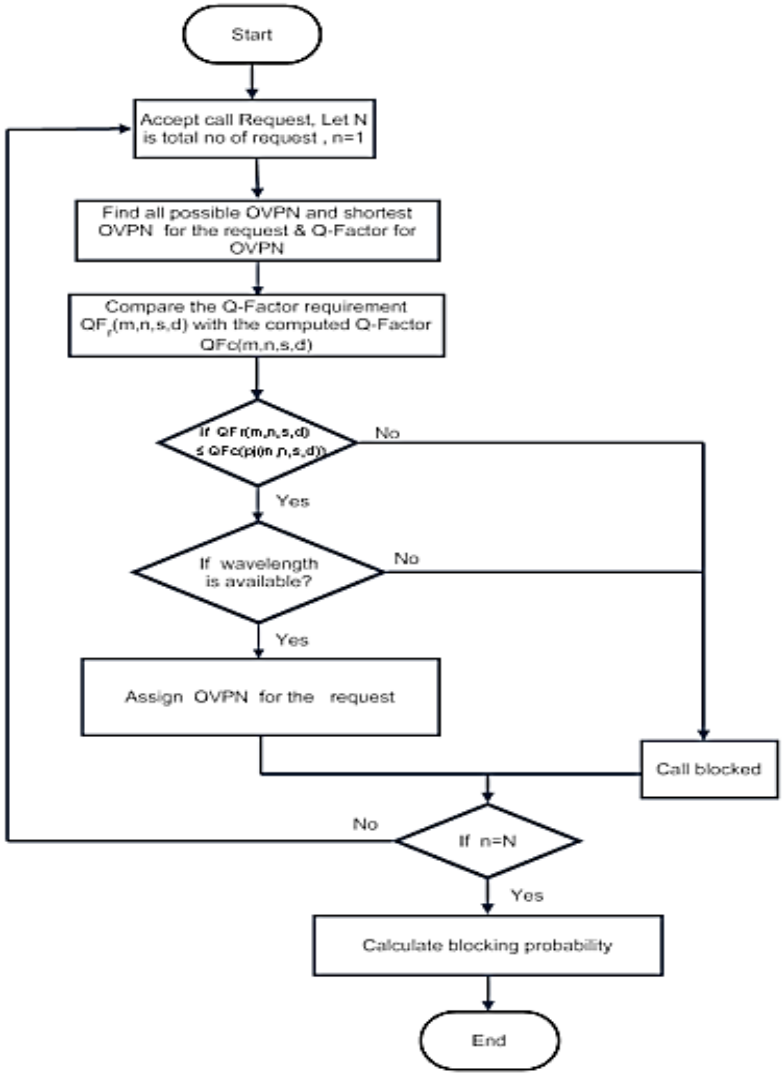

Fig 5.3 – Flow chart for connection setup mechanism using shortest path

OVPN Connection Setup Using Disjoint Paths

STEP 1: Find all possible OVPN connections for a connection request.

STEP 2: Find all disjoint OVPN connections from all possible OVPN connections and compute their Q-Factor.

STEP 3: Arrange all the disjoint OVPN connections in incremental order of Q-Factor. Let p is the total no of disjoint OVPN connections.

STEP 4: Compare the required Q-Factor value for a connection request with the Q-Factor values of all the connections arranged in STEP 3 one by one.

STEP 5: If it is satisfied then go to STEP 6, otherwise go to STEP 7.

STEP 6: Check whether the selected OVPN connection is busy or not. If busy the call will be blocked. Go to STEP 1 for next connection request, otherwise go to

STEP 7: Assign the selected OVPN connection for the requested connection. Go to STEP 1 for next connection request.

The flow chart for the above algorithm is:

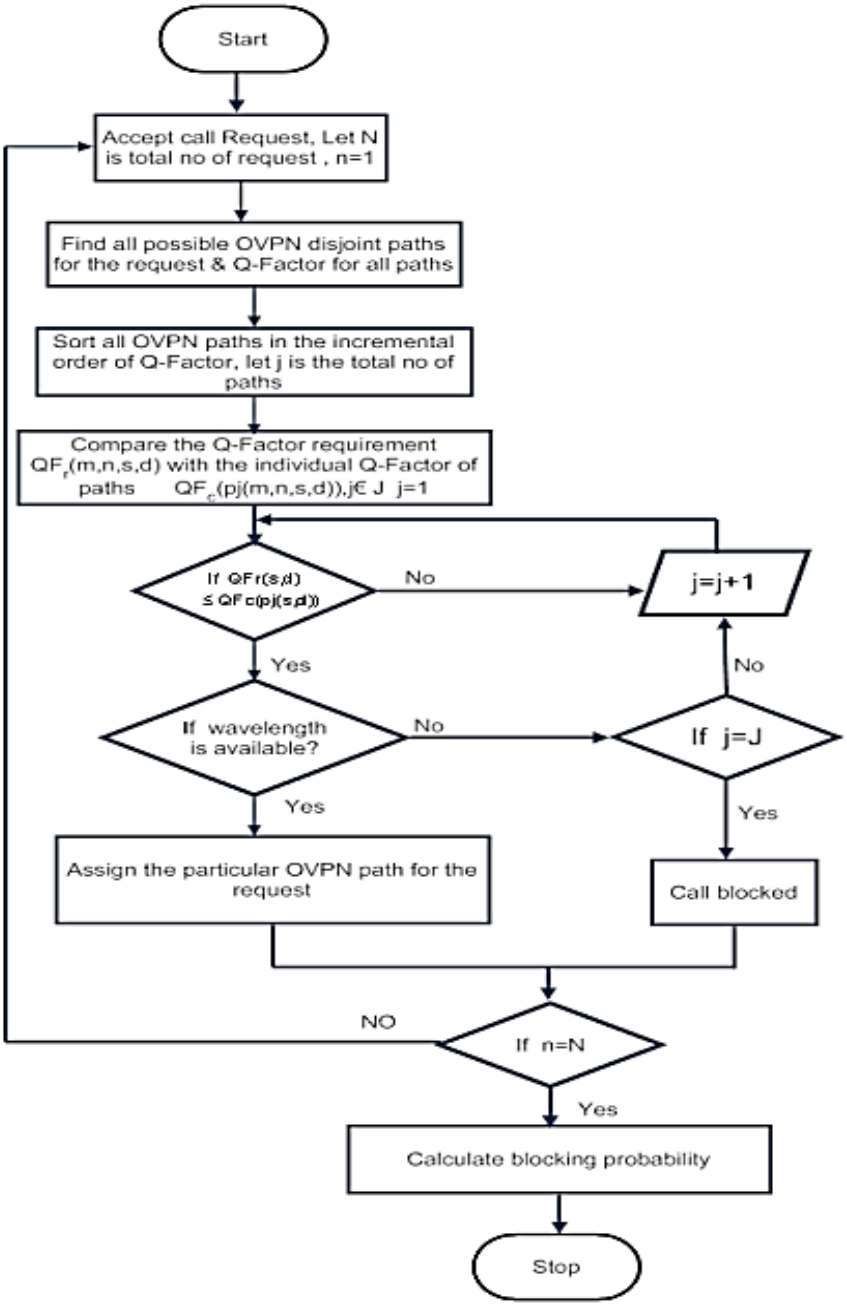

Fig 5.4 - Flow chart for connection setup mechanism using shortest path

The set of disjoint paths have been obtained using Suurballe's Algorithm. The disjoint paths are defined as the set of paths having no common vertex in the path from one common source to one common destination. We have examined the paths and computed the Q-factor for each possible path. In the simulation we have allotted paths from shortest

path set, disjoint path set, all possible path set and OBGP path set and compared the blocking probability in each case. OBGP path set can be found out assuming all connection in the network to be optical and applying BGP algorithm.

5.6 Simulation & Results

Network used for simulation is shown below:

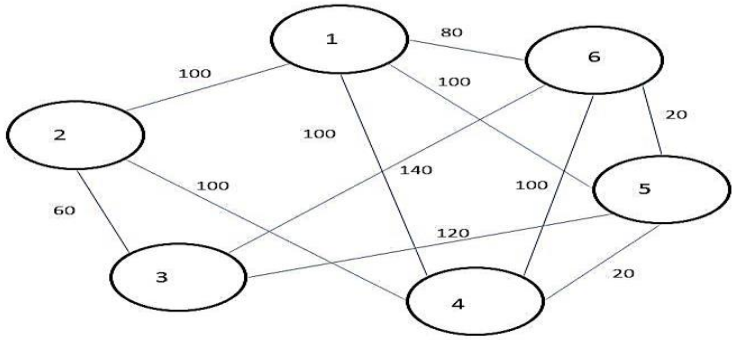

Fig 5.5 – Network topology used for simulation where link lengths are in kms

Assumptions:

Pulse Broadening factor (σ) = 0.1

Polarisation Mode Dispersion (D_{PMD}) = 0.2

Wavelength = 1280 nm.

The adjacency matrix and the link length matrix are given as inputs.

The adjacency matrix is

	r1	r2	r3	r4	r5	r6
r1	0	1	0	1	1	1
r2	1	0	1	1	0	0
r3	0	1	0	0	1	1
r4	1	1	0	0	1	1
r5	1	0	1	1	0	1
r6	1	0	1	1	1	0

Table 5.1 – Adjacency matrix for network model used for simulation

The link length matrix is

	r1	r2	r3	r4	r5	r6
r1	0	100	0	120	100	80
r2	100	0	60	100	0	0
r3	0	60	0	0	120	140
r4	120	100	0	0	20	100
r5	100	0	120	20	0	20
r6	80	0	140	100	20	0

Table 5.2 – Link length matrix for network model used for simulation

Simulation 1

(source, destination) = (1, 4)

The computed Q-factor of the all feasible paths

All possible paths						Q-factor
1	4	0	0	0	0	27
1	2	4	0	0	0	32
1	5	4	0	0	0	32
1	6	4	0	0	0	32
1	6	5	4	0	0	40
1	5	6	4	0	0	32
1	5	3	2	4	0	27
1	2	3	5	4	0	27
1	6	3	2	4	0	23
1	2	3	6	4	0	23
1	6	3	5	4	0	23
1	5	3	6	4	0	23
1	6	5	3	2	4	27
1	5	6	3	2	4	23
1	2	3	5	6	4	27
1	2	3	6	5	4	23

Table 5.3 – computed Q-factor for all possible paths for (s, d)=(1,4)

Connection request no. (crn)=5

Requested Q-factor (rqf)=20,25,30,35,45

Allotment from all possible paths

Crn	Rqf	Allotted path	Blocking Probability (in %)
1	20	1 6 3 2 4 0	20
2	25	1 4 0 0 0 0	
3	30	1 2 4 0 0 0	
4	35	1 6 5 4 0 0	
5	45	0 0 0 0 0 0	

Table 5.4 – path allotment from all possible paths for (1, 4) based on Q-factor

Allotted from disjoint paths

Crn	Rqf	Allotted path	Blocking Probability (in %)
1	20	1 4 0 0 0 0	40
2	25	1 4 0 0 0 0	
3	30	1 2 4 0 0 0	
4	35	0 0 0 0 0 0	
5	45	0 0 0 0 0 0	

Table 5.5 – path allotment from disjoint paths for (1, 4) based on Q-factor

Allotting shortest path

Crn	Rqf	Allotted path	Blocking Probability (in %)
1	20	1 4 0 0 0 0	60
2	25	1 4 0 0 0 0	
3	30	0 0 0 0 0 0	
4	35	0 0 0 0 0 0	
5	45	0 0 0 0 0 0	

Table 5.6 – path allotment from shortest paths for (1, 4) based on Q-factor

Alloting OBGP paths

Crn	Rqf	Allotted path	Blocking Probability (in %)
1	20	1 4 0 0 0 0	60
2	25	1 4 0 0 0 0	
3	30	0 0 0 0 0 0	
4	35	0 0 0 0 0 0	
5	45	0 0 0 0 0 0	

Table 5.7 – path allotment from OBGP optimal paths for (1, 4) based on Q-factor

The comparison of allotted Q-factor is:

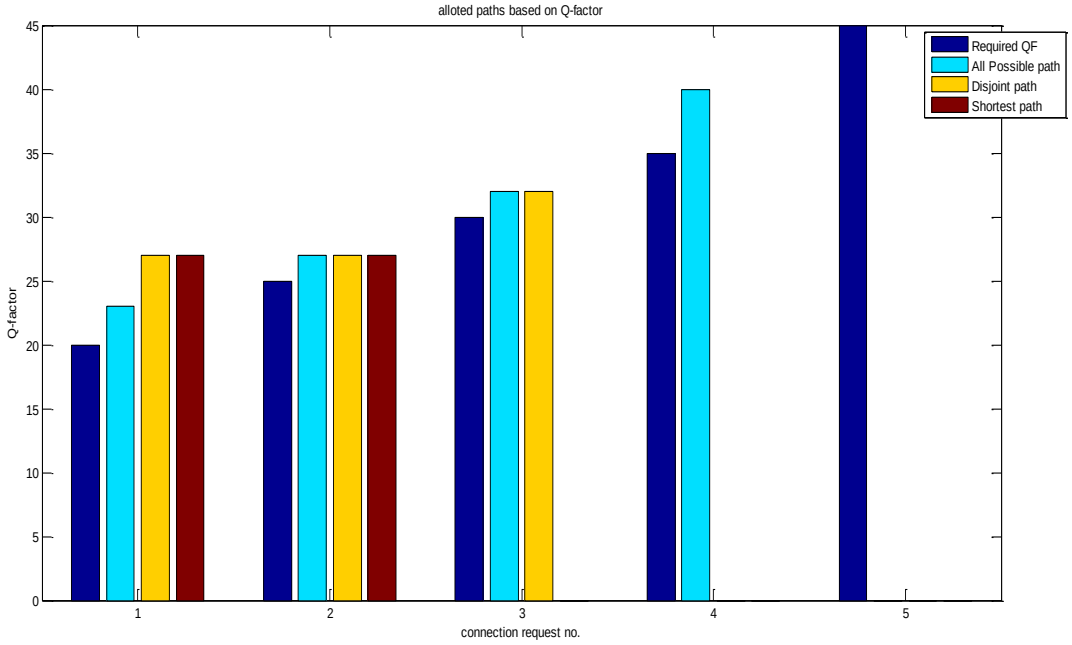

Fig 5.6 – Comparison of allotted Q-factor in simulation-1

As we can see from the graph, it describes the allotted path for different mechanisms based on required Q-factor. When the required Q-factor is low, path from any mechanism can be allotted. As it increases, then it becomes difficult to assign a path to the client.

In connection request no. 1, the required Q-factor is 20. Path (1-6-3-2-4) is having Q-factor 23, which is the lowest of the Q-factors of the paths that are greater than 20. So, path (1-6-3-2-4) is allotted.

In connection request no. 5, the required Q-factor is 45, which is higher than the available Q-factors of the path. So, no path is allotted to it. From these allotments we can calculate blocking probability.

From the fig 5.6 we can observe that shortest path allotment mechanism is providing more blocking than the disjoint path allotment mechanism.

The comparison of blocking probability:

for (s, d) = (1,4)

For a required Q-factor of the range = 20-45

For connection request no. – (5, 10, 15, 20)

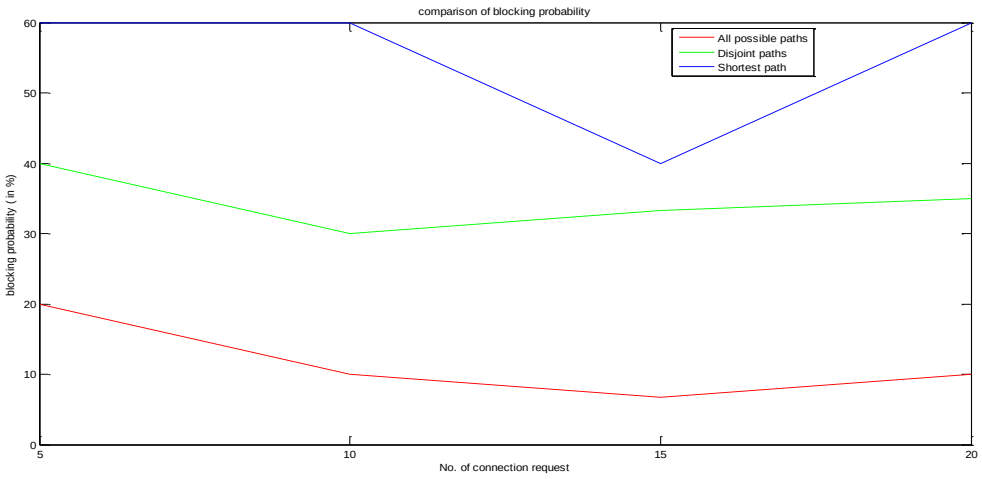

Fig 5.7 – comparison of blocking probability for all possible path, disjoint path, shortest path in simulation-1

From the graph, it is learned that when allotting paths from all possible paths and disjoint path set the blocking probability decreases significantly as compared to when assigning the shortest path.

Simulation 2

(source, destination) = (3, 6)

The computed Q-factor of the all feasible paths

All possible paths						Q-factor
3	6	0	0	0	0	23
3	5	6	0	0	0	27
3	5	4	6	0	0	27
3	2	4	6	0	0	32
3	5	1	6	0	0	27
3	2	1	6	0	0	32
3	2	4	1	6	0	27
3	2	1	4	6	0	27
3	2	1	5	6	0	32
3	5	4	1	6	0	27
3	5	1	4	6	0	27
3	2	4	5	6	0	32
3	5	4	2	1	6	27
3	5	1	2	4	6	27
3	2	4	5	1	6	32
3	2	4	1	5	6	27
3	2	1	5	4	6	32
3	2	1	4	5	6	27

Table 5.8 - computed Q-factor for all possible paths for (s, d)=(3, 6)

Connection request no. (crn)=5

Requested Q-factor (rqf)=20,24,28,32,36

Allotted from all possible paths

Crn	Rqf	Allotted path	Blocking Probability (in %)
1	20	3 6 0 0 0 0	20
2	24	3 5 6 0 0 0	
3	28	3 2 4 6 0 0	
4	32	3 2 4 6 0 0	
5	36	0 0 0 0 0 0	

Table 5.9 – path allotment from all possible paths for (3, 6) based on Q-factor

Allotted from disjoint paths

Crn	Rqf	Allotted path	Blocking Probability (in %)
1	20	3 6 0 0 0 0	20
2	24	3 5 6 0 0 0	
3	28	3 2 1 6 0 0	
4	32	3 2 1 6 0 0	
5	36	0 0 0 0 0 0	

Table 5.10 – path allotment from disjoint paths for (3, 6) based on Q-factor

Allotted from shortest path

Crn	Rqf	Allotted path	Blocking Probability (in %)
1	20	3 6 0 0 0 0	60
2	24	3 5 6 0 0 0	
3	28	0 0 0 0 0 0	
4	32	0 0 0 0 0 0	
5	36	0 0 0 0 0 0	

Table 5.11 – path allotment from shortest paths for (3, 6) based on Q-factor

Allotted from OBGP path

Crn	Rqf	Allotted path	Blocking Probability (in %)
1	20	3 6 0 0 0 0	80
2	24	0 0 0 0 0 0	
3	28	0 0 0 0 0 0	
4	32	0 0 0 0 0 0	
5	36	0 0 0 0 0 0	

Table 5.12 – path allotment from OBGP optimal paths for (3, 6) based on Q-factor

The comparison of allotted Q-factor is:

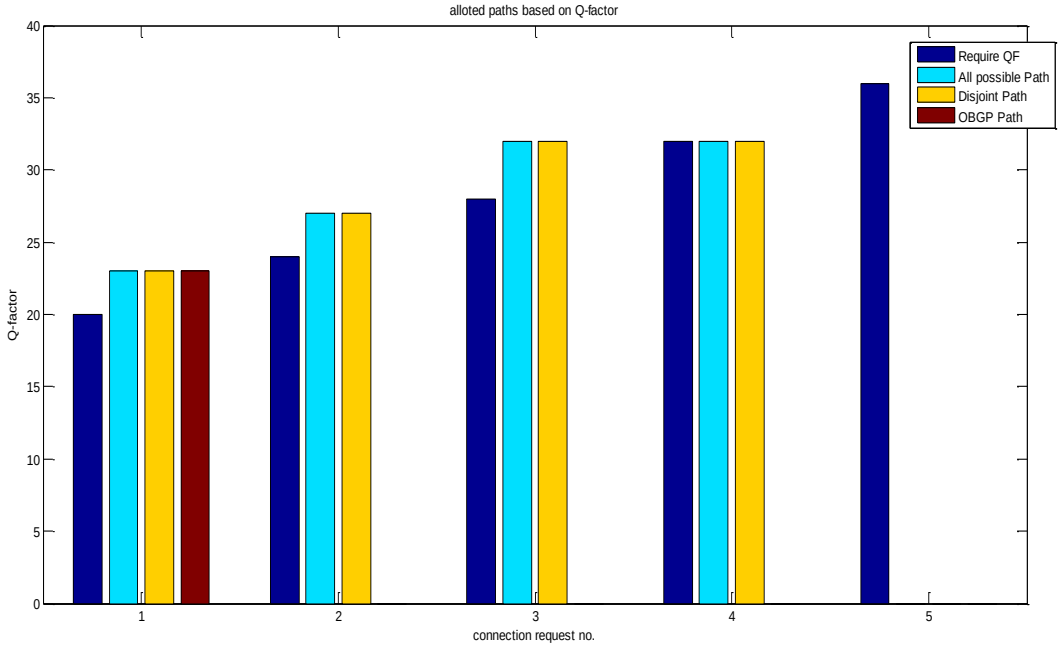

Fig 5.7 – Comparison of allotted Q-factor in simulation-2

As we can see from the graph, it describes the allotted path for different mechanisms based on required Q-factor. When the required Q-factor is low, path from any mechanism can be allotted. As it increases, then it becomes difficult to assign a path to the client.

In connection request no. 1, the required Q-factor is 20. Path (3-6) is having Q-factor 23, which is the lowest of the Q-factors of the paths that are greater than 20. So, path (3-6) is allotted.

In connection request no. 5, the required Q-factor is 36, which is higher than the available Q-factors of the path. So, no path is allotted to it. From these allotments we can calculate blocking probability.

From the fig 5.7 we can observe that OBGP path allotment mechanism is providing more blocking than the disjoint path allotment mechanism. The reason we can assume that while finding BGP paths the algorithm doesn't consider the QoS parameters.

The comparison of blocking probability

for (s, d) = (3, 6)

For a required Q-factor of the range = 20-40

For connection request no. – (5, 10, 15, 20)

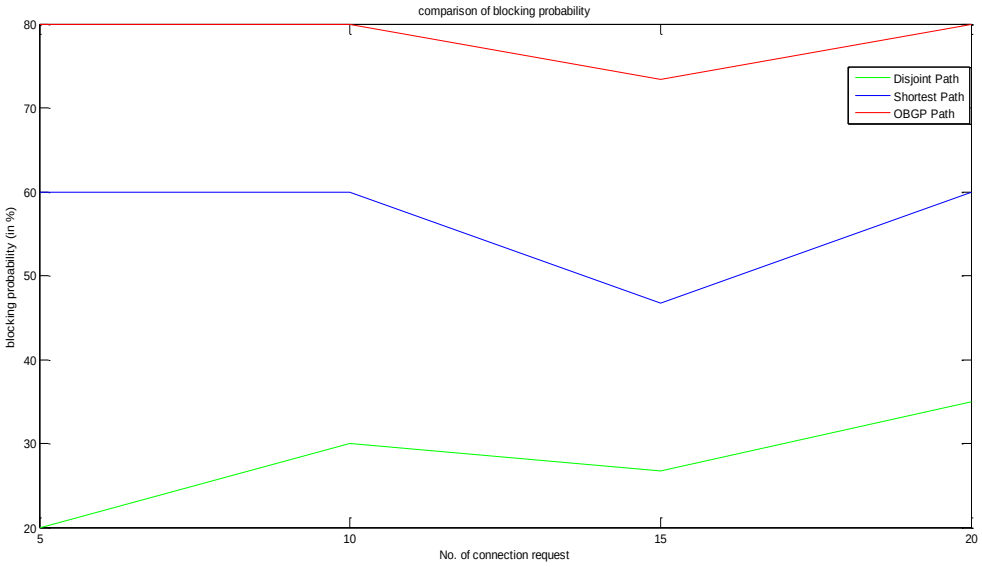

Fig 5.7 – comparison of blocking probability for all possible path, disjoint path, shortest path in simulation -2

From the graph, we can observe that the path allotting mechanism which involves allotment from OBGP path provides significant amount of blocking rather than the disjoint path or shortest path provisioning.

5.7 Conclusion

We have discussed about the RWA (Routing and Wavelength Assignment) function of the OVPN connection setup. Choosing the shortest path between two nodes as an optimal path is not a smart solution always. We have assigned path as per the q-factor requirement of the application, which is calculated from bandwidth requirement and delay of the link. Here we have considered the effect of PMD (Polarization Mode Dispersion) which is the prominent factor affecting the speed of fiber. By assigning paths from the all possible path set and disjoint path set, the blocking probability has been decreased significantly. This mechanism can provide a better QoS to the end-to-end customers.

Chapter 6: Conclusion

6.1 Conclusion

In this thesis, we have discussed about BGP protocol and its extension OBGP protocol. We have studied the path attributes for finding the optimal path in the network. The network has been implemented using MATLAB programming and simulation has been done. We have also studied OBGP and QoS parameters and their role in routing function in network.

An OVPN model is studied and implemented. A comparison has been done between different path allotting mechanisms such as all possible path set, disjoint path set, shortest path, OBGP path. The blocking probability has been the comparison criteria. In the path provisioning, the decisions are made on the basis of required Q-factor and computed Q-factor.

From the project, it is learned that when optimal path is to be found out, assigning the shortest path or the OBGP path is not a smart solution always. The paths should be assigned taking the QoS parameters into consideration. Here we have taken the QoS parameters: bandwidth and delay requirement in terms of Q-factor. By assigning paths from all possible path set and disjoint path set, we observe that the blocking probability decreases significantly.

6.2 Future Work

In this thesis we have considered the path between two nodes in the network. So we have considered the QoS parameters such as: bandwidth and delay requirements. We have not taken into consideration about how the packets are moving in a network. Also the QoS parameters like reliability and jitter which depend on the movement of packets in the network are to be studied. A mechanism should be suggested which can take all the QoS parameters into consideration. Also the path finding process through OBGP protocol is to be advanced.

References

[1] S. K. Das, Dhanya V. V., S. K. Patra, QoS Based OVPN Connection Set up and Performance Analysis, E-ISSN: 2224-2864, Issue 8, Volume 11, August 2012.

[2] S. K. Das, Route Slection and VPN creation based on MPLS-BGP Techniques, A Thesis submitted for the Master of Science (Engineering).

[3] S. K. Das, S. K. Naik and S. K. Patra, "Fiber Material Dependent QoS Analysis and OVPN Connection Setup over WDM/DWDM Networks", in IEEE TENCON, pp. 521-525,2011

[4] S. Jeong, C. HyunYoun, M. Kang, K. Seon Min Hyun Ha Hong, and Hae Geun Kim, Optical BGP Routing Convergence in Lightpath Failure of Optical Internet, ETRI Journal, Volume 24, Number 2, April 2002.

[5] Internetworking Technology Overview, June 1999, Chapter -35, Border Gateway Protocol, published on pulsesupply.com.

[6] J. Wu, M. Savoie, S. Campbell, H. Zhang, G. V. Bochmann and B. Arnaud, "Customer-managed end-to-end lightpath provisioning", INTERNATIONAL JOURNAL OF NETWORK MANAGEMENT, Int. J. Network Mgmt 2005; 15: 349–362

[7] M. J. Francisco, S. Simpson, L. Pezoulas, C. Huang, I. Lambadaris, "Interdomain Routing In Optical Networks", Dept. Systems and Computer Engineering, Advanced Optical Networks Laboratory, Carleton University, 1125 Colonel By Drive, Ottawa, ON K1S 5B6

[8] M. Blanchet, F. Parent, and B. St-Arnaud, "Optical BGP (OBGP): IDRA lightpath provisioning," IETF draft, ietf-draft-parent-obgp-01, Mar. 2001.

[9] J. M. Kim, O. H. Kang, J. Jung, S. U. Kim, Control Mechanism for QoS Guaranteed Multicast Service in OVPN over IP/GMPLS over DWDM, Journal of Communications, Vol.2 , No.1, 2007, pp. 44-51.

[10] S. H. Bouk, I. Sasase, S. H. Ahmed, and Nadeem Javaid, "Gateway Discovery Algorithm Based on Multiple QoS Path Parameters Between Mobile Node and Gateway Node", JOURNAL OF COMMUNICATIONS AND NETWORKS, VOL. 14, NO. 4, AUGUST 2012.

[11] A. Leiva, J. M. Finochietto, B. Huiszoon, V. Lopez, M. Tarifeno, J. Aracil, A. Beghelli, Comparison in Power Consumption of Static and Dynamic WDM Networks, Optical Switching and Networking, Vol.8, No.3, 2011, pp. 149-161.

[12] R. Yousif,A. B. Mond, M. K. Abdullah, K. Seman, M. D. Baba, Design Considerations For Efficient multicast WDM Network Scalable Architecture, Transaction on Network and Communication, Vol.2, 2011, pp. 64-72.

[13] F. L. Verdi, M. F. Magalhaes, E. Cardozo, E. R. M. Maderia, A. Welin, A Service Oriented Architecture –Based Approach for interdomain Optical Network Services, Journal of Network and systems Management, Vol.15, No.2, 2007, pp. 288-309.

[14] C. V. Saradhi, S. Subramaniam, Physical Layer Impairment Aware Routing (PLIAR) In WDM Optical Networks:issues and Challenges, IEEE Communication Surveys & Tutorials, Vol.11, No.4, 2009, pp. 109-130.

[15] Y. Huang, J. P. Heritage, B. Mukherjee, Connection Provisioning with Transmission Impairment Consideration in Optical WDM Networks with High-Speed Channels, Journal of Light wave technology, Vol.23, No.3, 2005, pp. 982-993.

[16] A. S. Tanenbam, Computer Networks, 4th edition, Chapter 5,page 290-320.

[17] S. Sangli, D. Tappan, Y. Rekhter, "BGP extension community attribute", lETF RFC 4360, February 2006.

[18] S. Jeong, Analysis of BGP Routing Convergence Using Inter-AS Relationship, M.S. Thesis, Information and Communications University, Korea, June 2001.